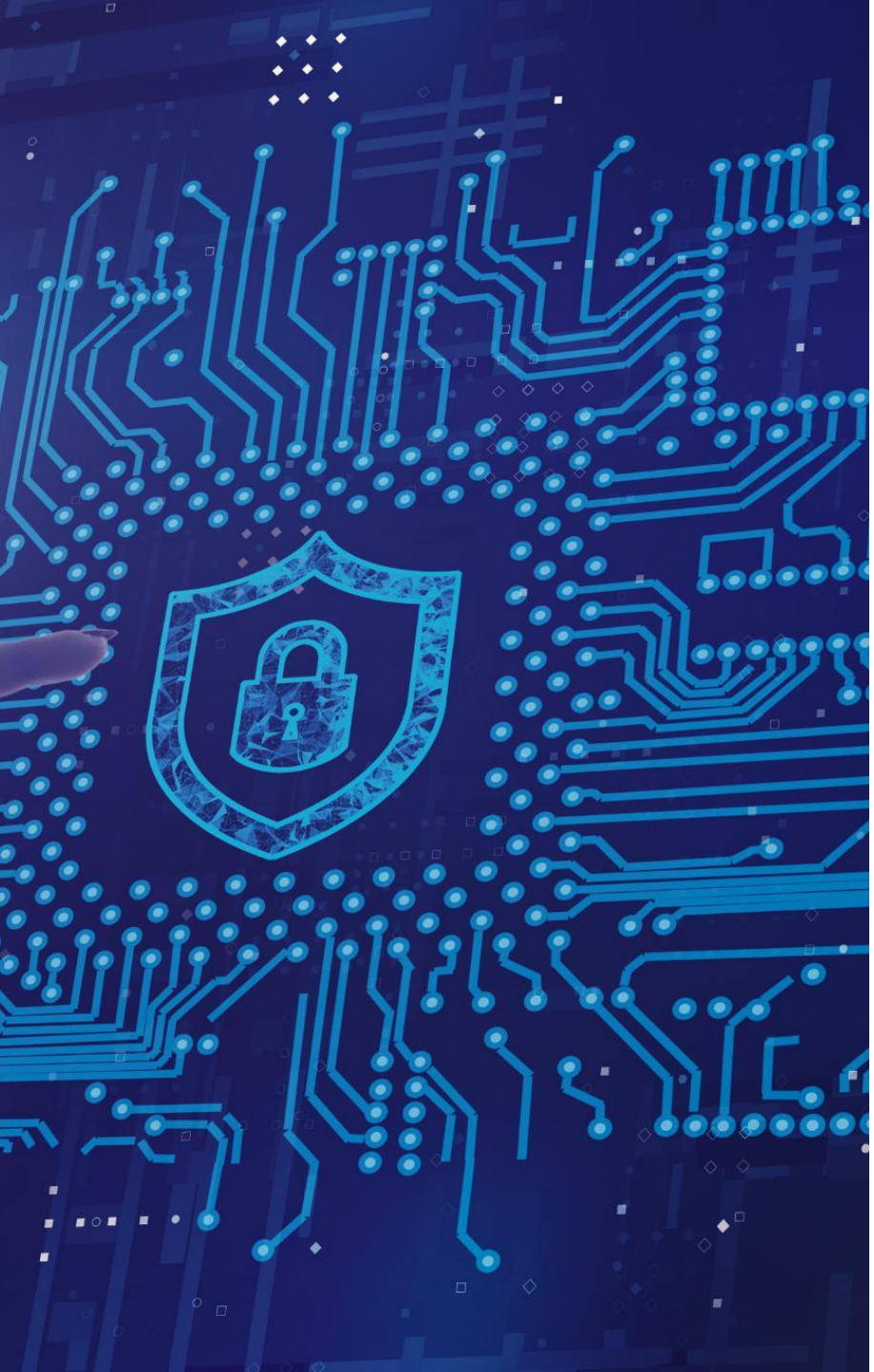
Player Infrastructure for Attack and Defense CTF Competitions

ANDREA ARTIOLI, EDOARDO TORRINI, LORENZO ROSSI, FRANCESCO MECATTI, MAURO ANDREOLINI

University of Modena and Reggio Emilia

{name.surname}@unimore.it



Background & Motivation

What are CTFs?

Capture The Flag, cybersecurity competitions where points are earned exploiting systems

Educational Value of CTFs

CTF competitions effectively develop offensive and defensive cybersecurity skills.

CTF Competition Formats

Jeopardy, Boot-to-Root, and Attack-Defense.

What Are Attack & Defense CTFs?

Attack-Defense Format Focus

Attack-Defense CTFs require both offensive and defensive skills simultaneously.

Complexity of A/D CTFs

Attack and Defense CTFs challenge newcomers with complex player infrastructure needs.

Cyberchallenge.it

What is Cyberchallenge.it?

Italy's national program for training young (16-24) cybersecurity talents.

Phases

Participants must pass a pretest, complete intensive training, and succeed in a Jeopardy-style CTF.

Final challenge

The competition culminates in an in-person Attack-Defense CTF held in Turin.

Final Attack-Defense in numbers

Participants:

40 teams

240 people

Challenge:

4 services

8+ vulnerabilities (crypto, web, binary, misc)

Flags:

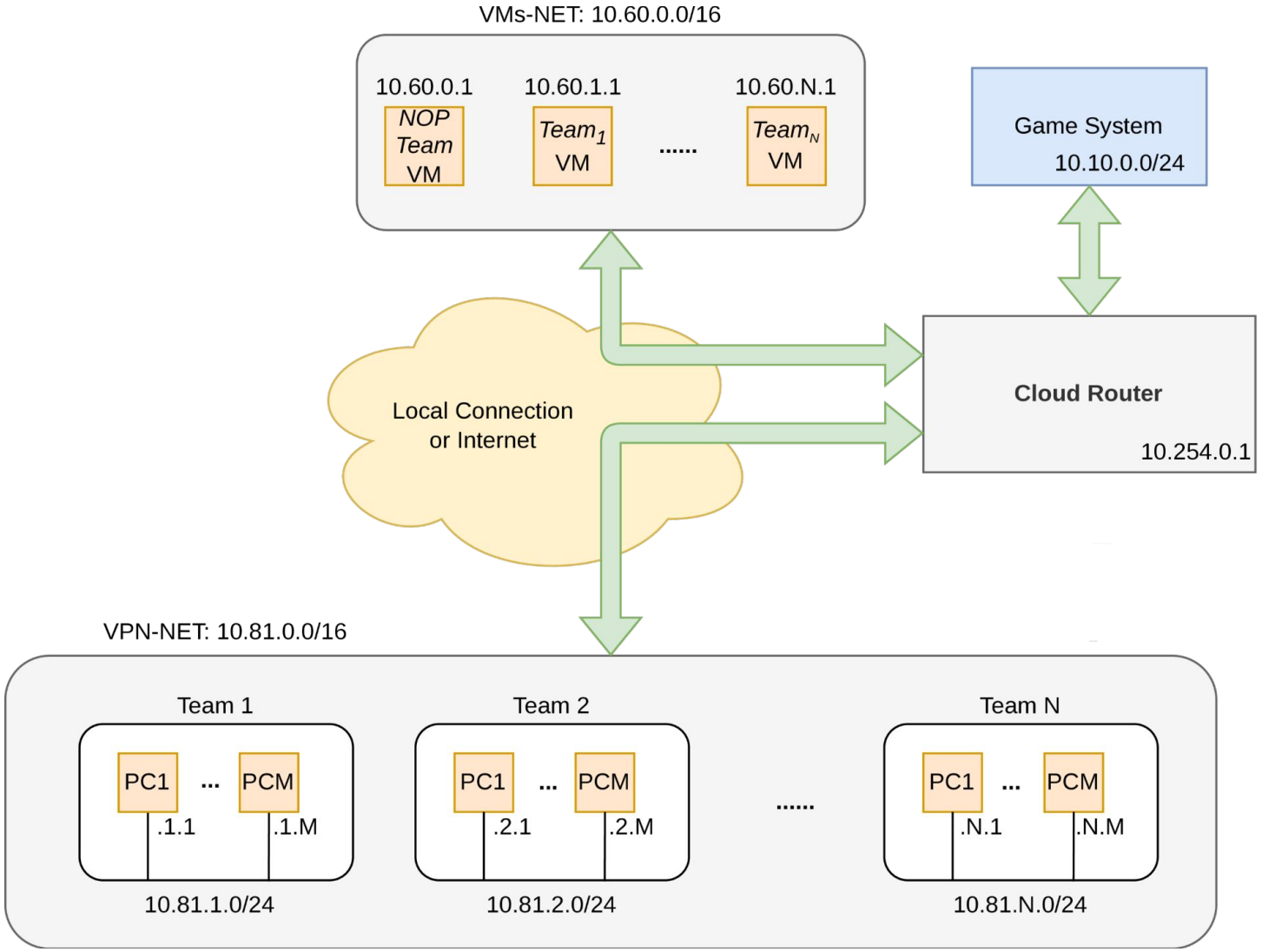
66.830 unique flags

378.332 stolen flags

Data:

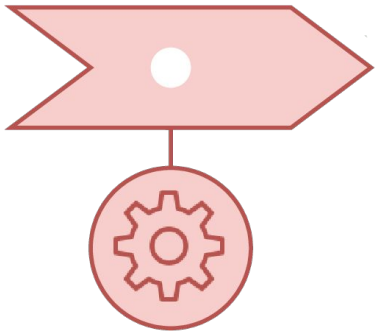
1.5TB+ of traffic in 8 hours

Final A/D - network infrastructure



Final A/D - game phases

Grace Period

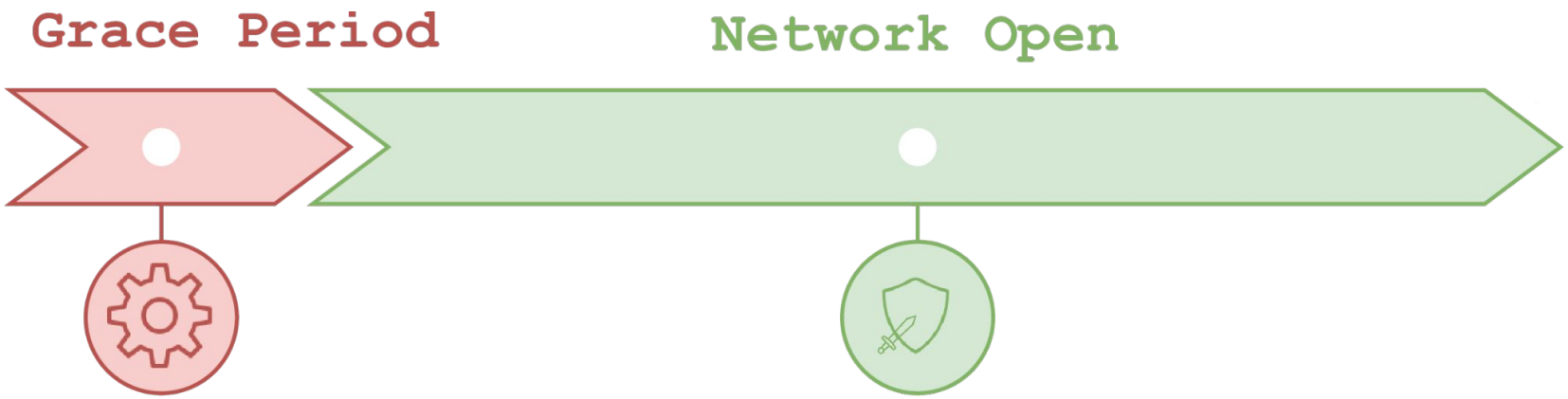


The Network is **closed**

Teams can only access their **vulnbox**

Teams use this period to **set up their own infrastructure**

Final A/D - game phases

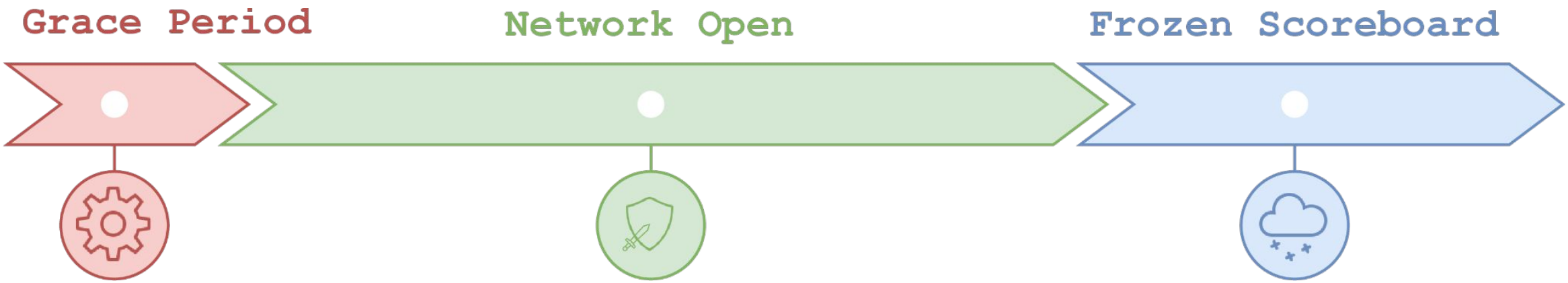


The Network is **open**

The teams launch their exploits and defend their services

The **Gamesystem** launch **checkers** and calculate points every tick

Final A/D - game phases



The Network is **open**

The teams launch their exploits and defend their services

The **Gamesystem** launch **checkers** and calculate points every tick

Player side infrastructure

Definition

Tools deployed by player in order to facilitate administration, attack and defense operations.

Desired functionalities

- Automatic deployment
- Proxy with filtering capabilities
- Traffic monitor
- Flag/exploit farmer
- Analytics

Our contributions

Novel player side infrastructure

First complete and open-source player side infrastructure.

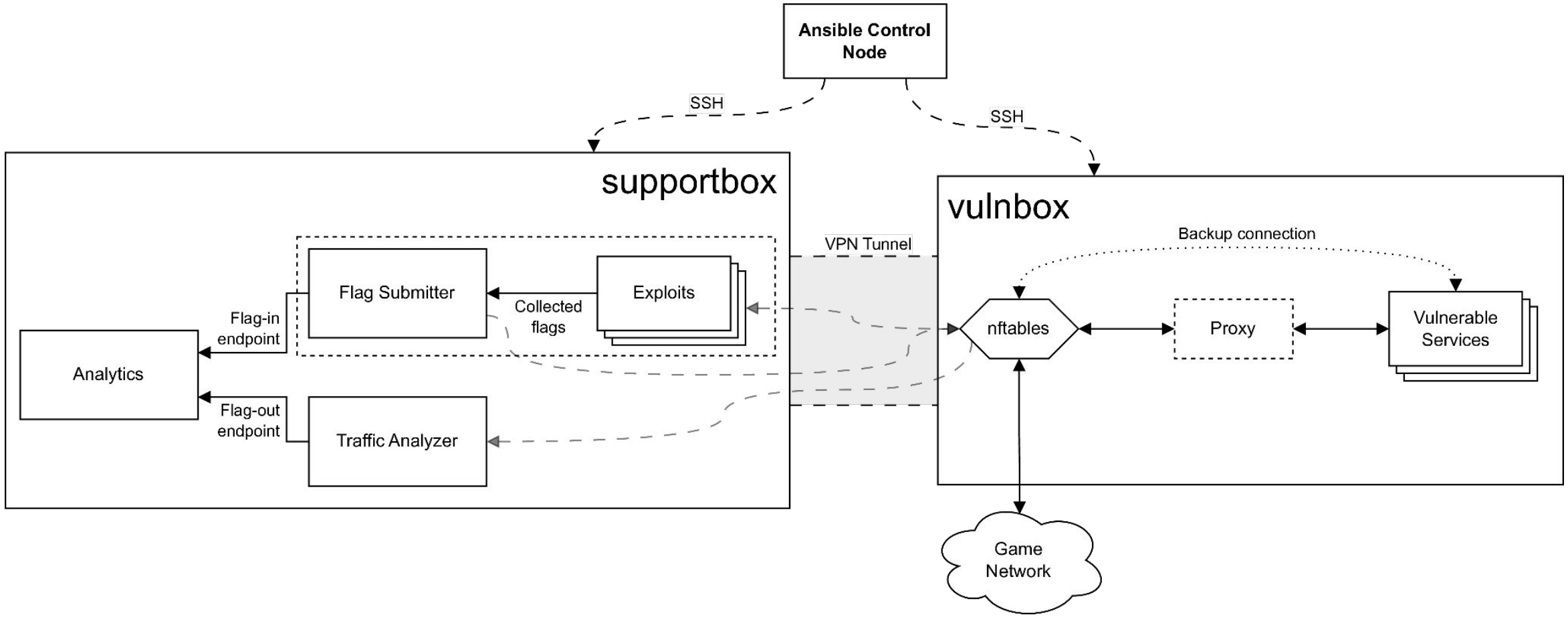
Core Functional Components

- Custom deployment tool
- Custom proxy
- Network monitor (Packmate)
- Flag submitter (S4DFarm)
- Custom analytics dashboard

Supportbox for Performance

A supportbox offloads resource-intensive tasks, optimizing performance on the constrained vulnbox.

Proposed Infrastructure – Overview



Evaluation

Real world testing

Participation at 5 A/D CTFs

- CCIT{25,24,23}
- FaustCTF23
- SaarCTF23

Latency Assessment

Stress tests measured round-trip time showing minimal latency increase under filtering scenarios.

Failover Resilience

Failover tests simulated crashes measuring the downtime before original connections are restored.

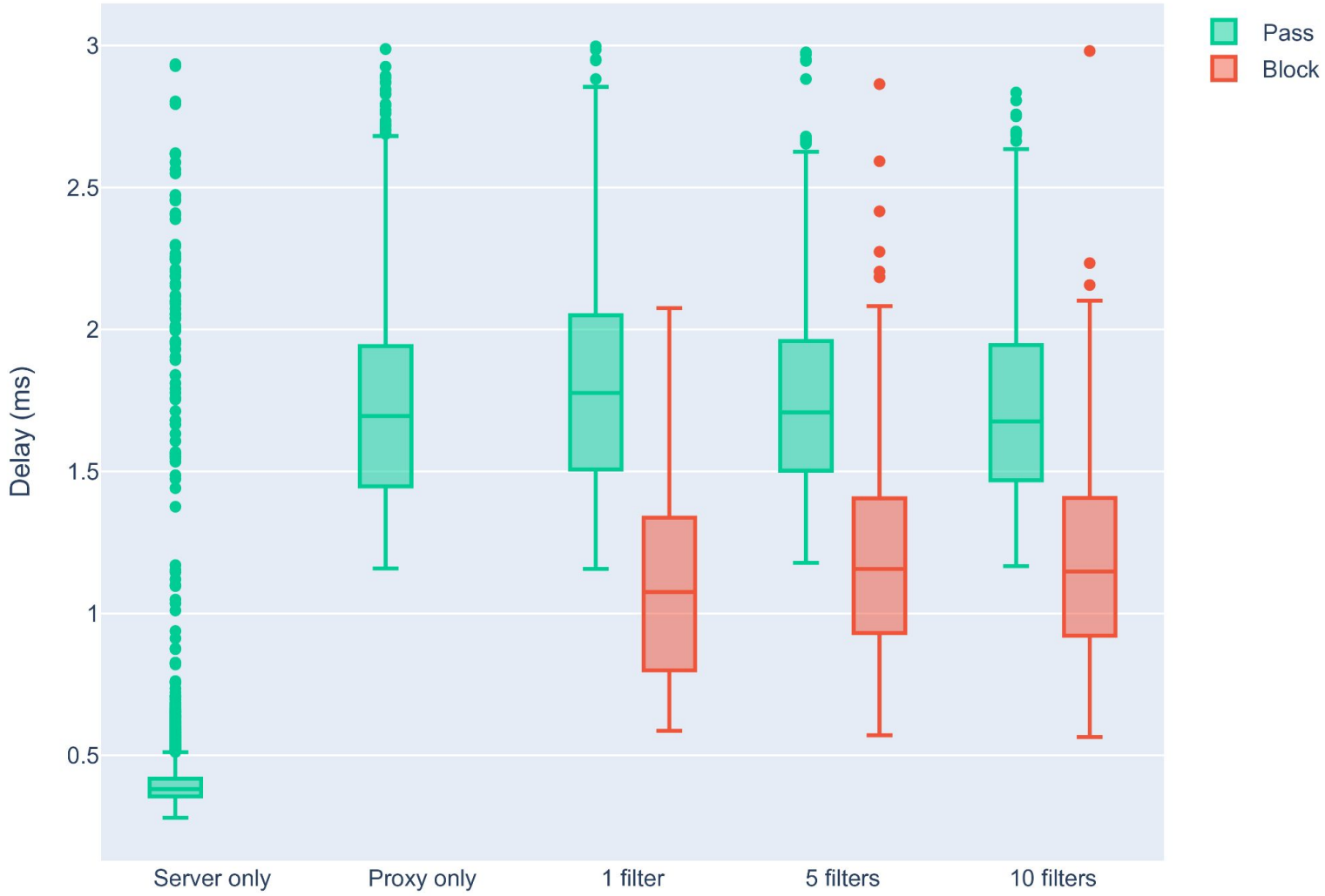
Latency Assessment

Synthetic RTT measurements

- Synthetic workload
  - 6000 requests
- Different proxy configurations

Objective

Measure the delay introduced by proxy and filters.



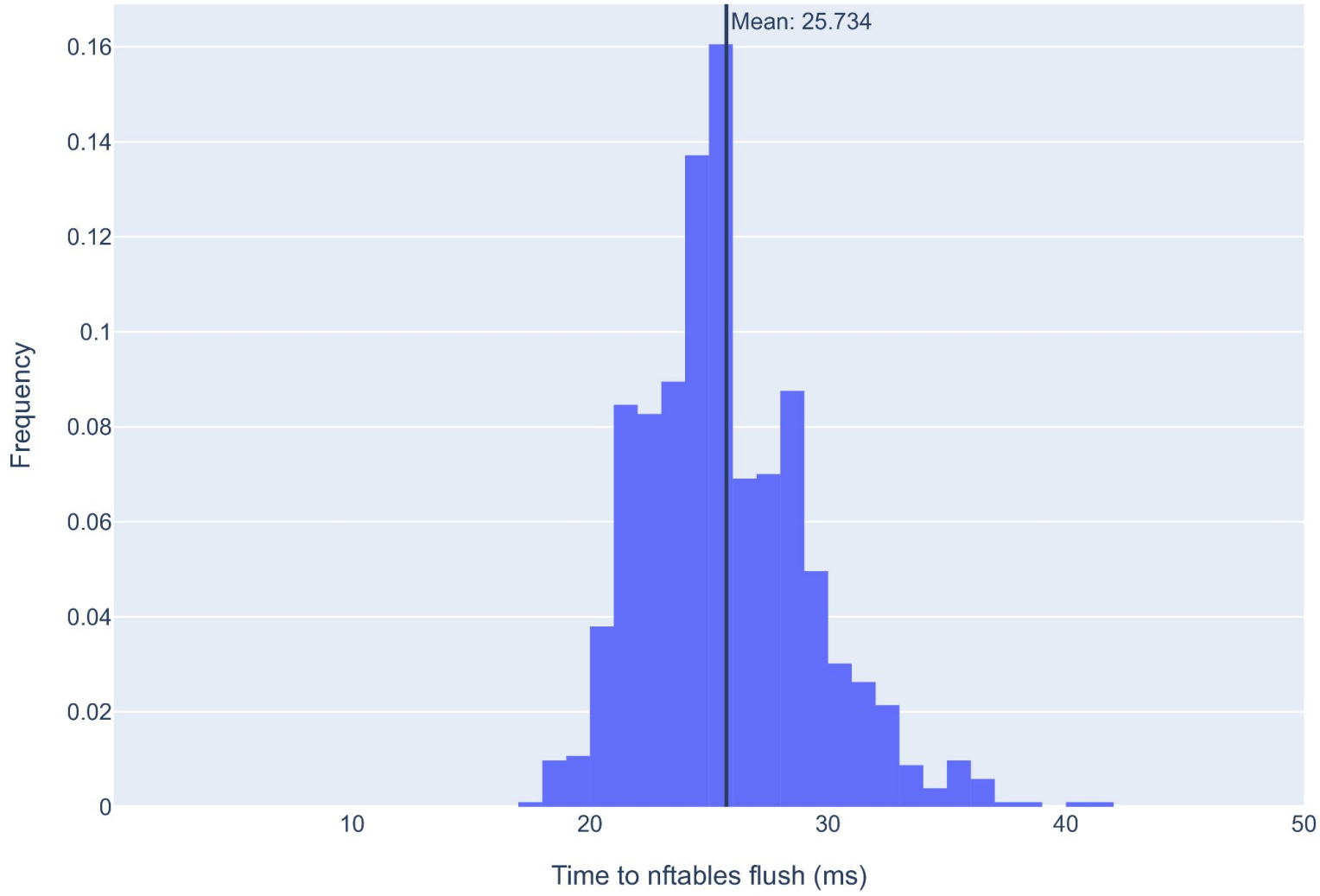
Failover Resilience

Time to restore original connections

- EBPF probes
- Send KILL signal to the proxy
  - 1000 samples

Objective

Measure the downtime in case of proxy failure.



Related work

A/D Community

Work	Traffic Monitor	Firewall or Proxy	Exploit Runner	Unified Analytics	Automatic Deploy	Supportbox Support
ByteTheCookies [20], [21]			✓	✓	✓	
Polytechnic of Bari [22]–[24]	✓	✓	✓			
TeamEurope [25]	✓	✓	✓			✓
Team France [26]	✓					
Team Norway (Cyberlandslaget) [27]			✓			
Our work	✓	✓	✓	✓	✓	✓

Conclusion & Future Work

Novel Player-side A/D Infrastructure

The system provides a complete automated setup for administration, offensive and defensive operations.

Evaluation

Tested in real competitions, measured RTT delay, downtime while backing up connections.

Future Enhancements

Plans include integrating machine learning for traffic analysis and modular tool selection during deployment.

Collaboration

andrea.artioli@unimore.it